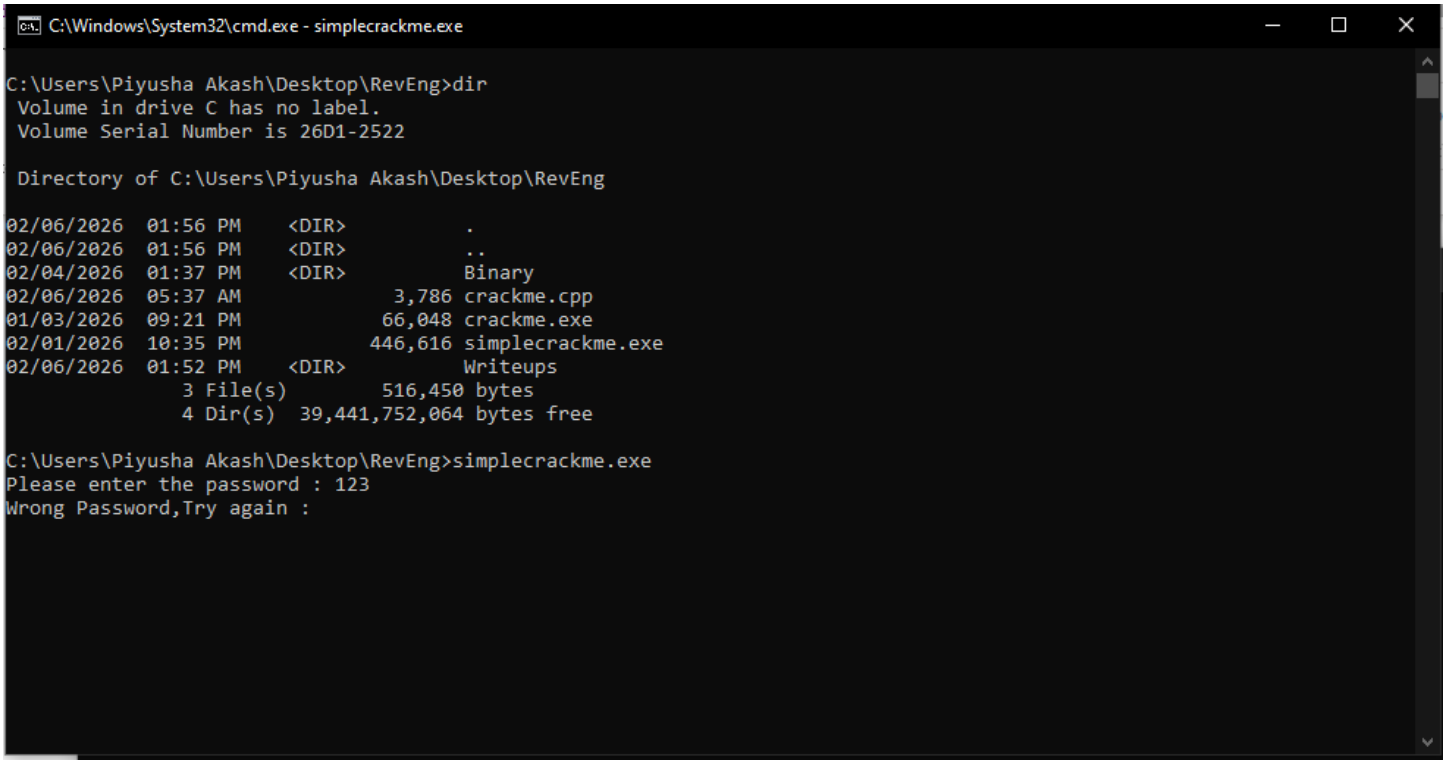
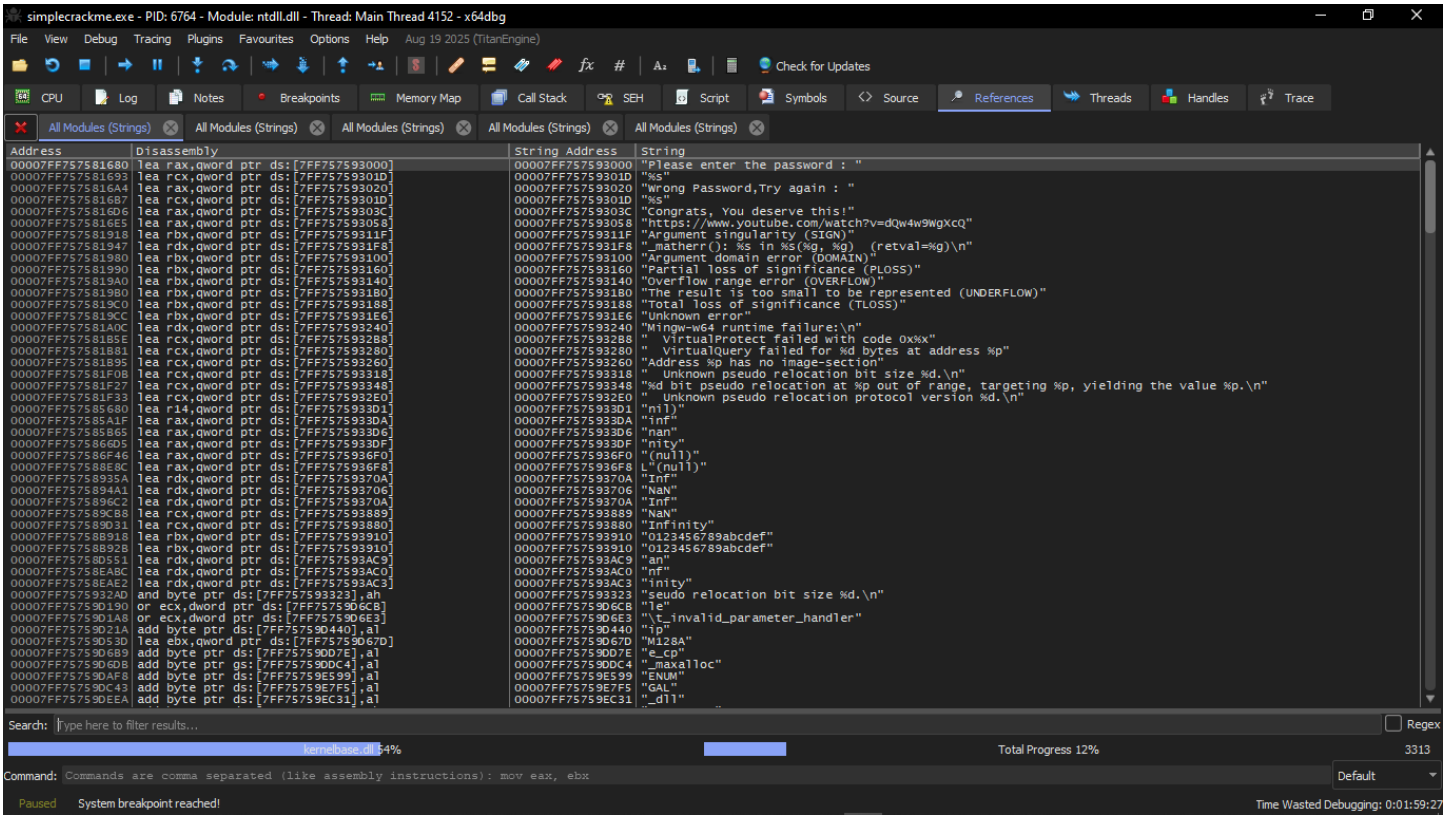
SIMPLECRACKME.exe | crackmes.one

This is a simple crackme program that created for practice reverse engineering. But this is bit hard because not like previous one (acrackme.exe), This crackme haven't password as plain text. We need to patch this to get secret. So, let's get started.



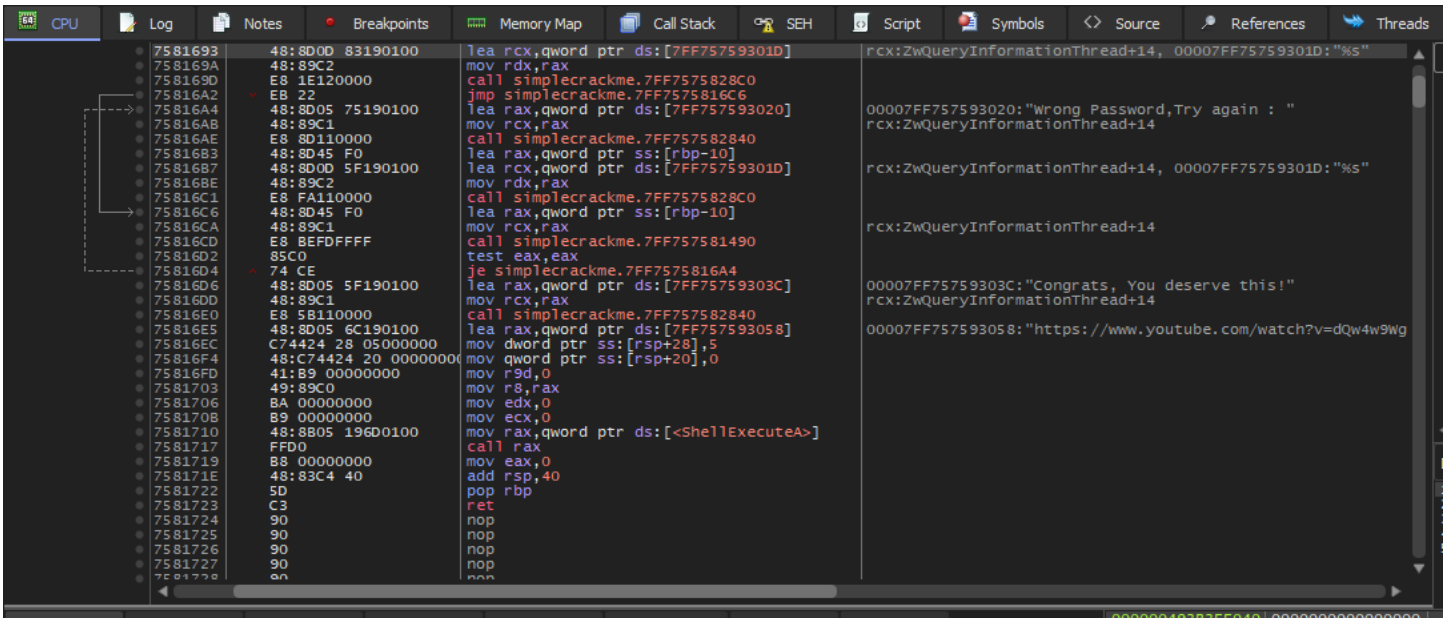
So, as you can see, it will ask for password. So, I just entered "123" as a password and it is wrong and it will return "Wrong Password, Try again:" as the result. So, let's put this in to **x64 dbg** for analyze.



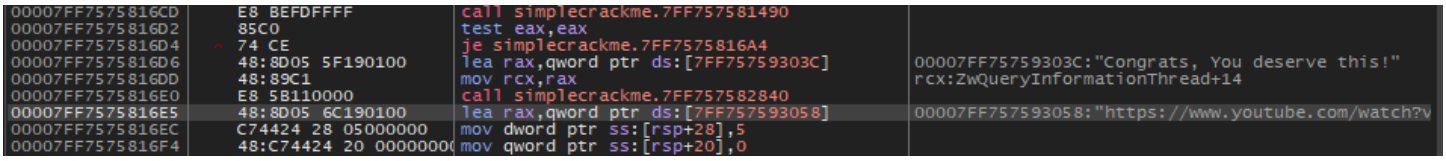
So, as you can see there is no any password as plaintext. We can see string "**Please enter the password:**" and input for password **(%s | %s is format specifier in C for string**) for example,

```
char password[10] = "";

printf("Please enter the password");

scanf("%s", password); //(This is an example code.)
```

So, let's jump to this section. I will double click this string and goes to disassembled section to looking for Assembly instructions.



So, you can see, the disassembled section. So, in that case, I don't care what is the password. As a hacker I have to make this program obey to my instructions. So, I just re-assemble the program by editing assembly instructions. Look at this image,



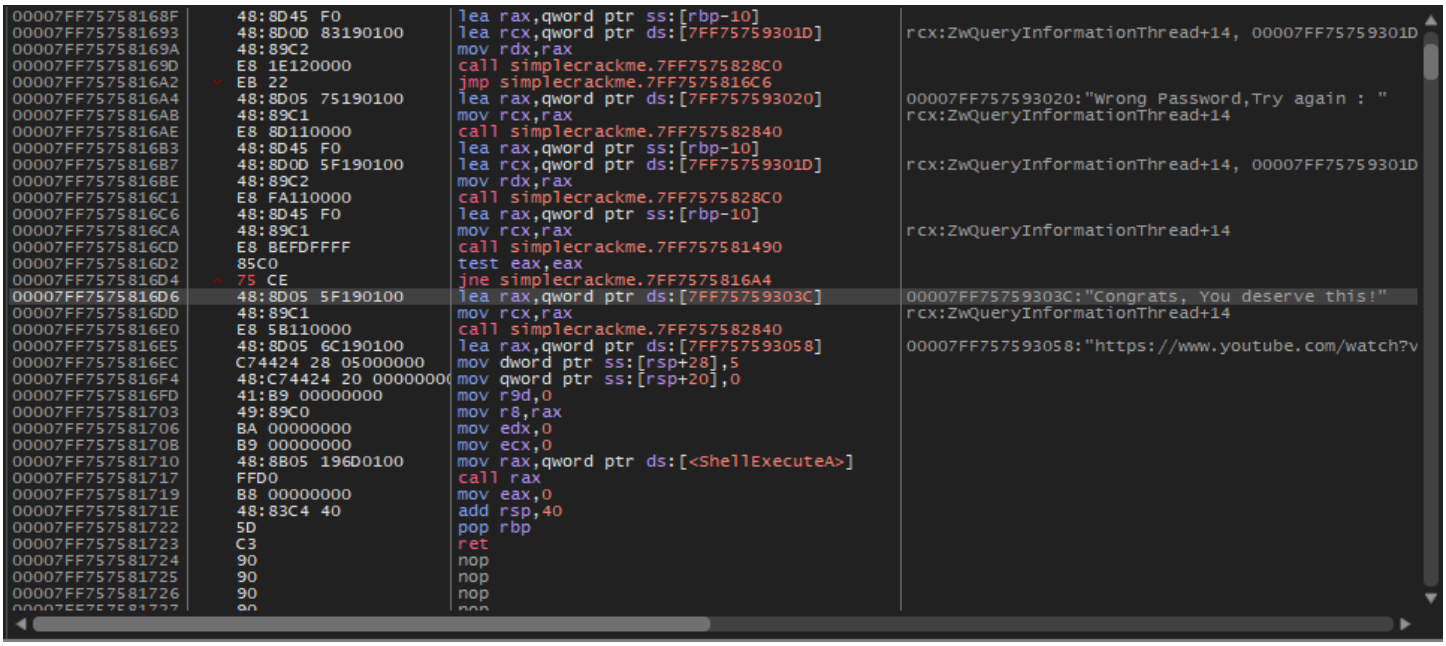
You can see a sting like "**Congrats, You deserve this!**". And you can see above to this string a "**je**" instruction. **JE** or **JZ,** whatever, It's meaning is "**Jump if equal**". So, according to the assembly instruction, If our password is true, Jump to

```
lea rax,qword ptr ds:[7FF75759303C]          00007FF75759303C:"Congrats, You deserve this!"
```

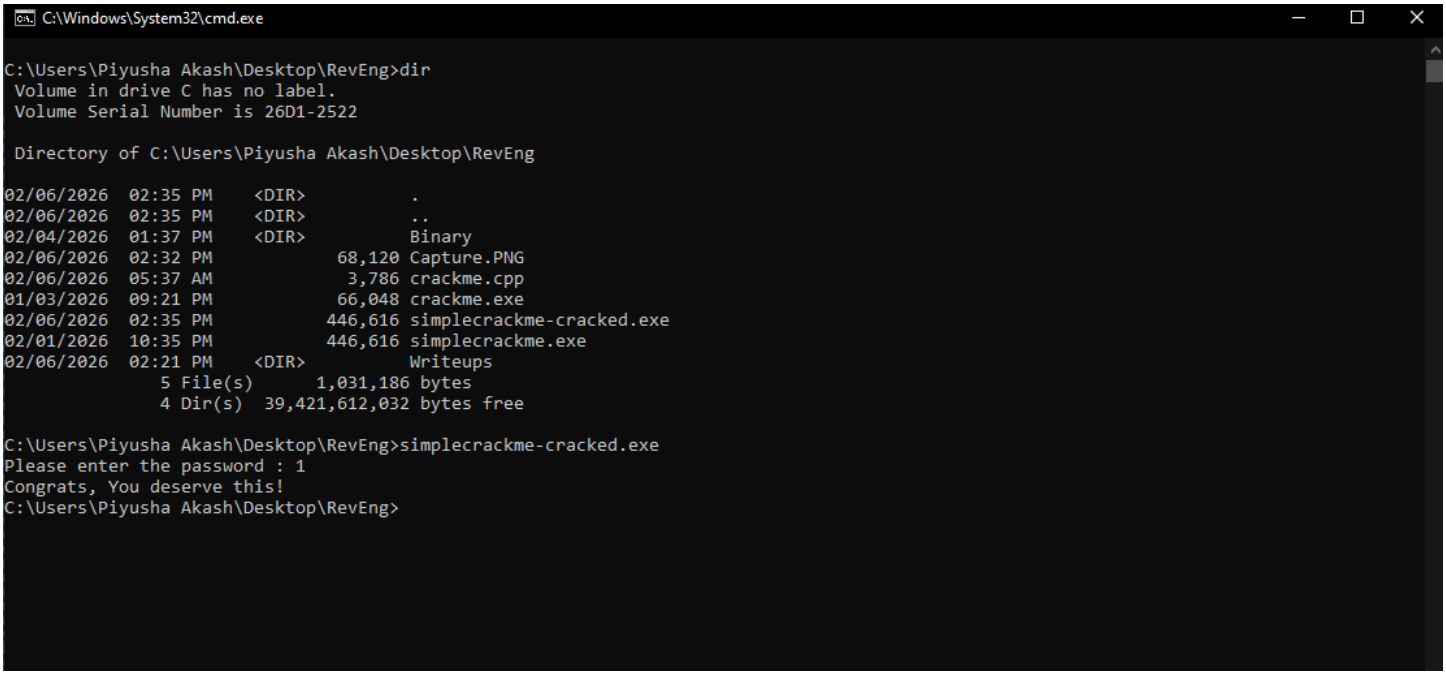
So, what if we can change the logic to if our password is wrong, jump to given memory address. So, let's try. I will change **je** to **jne**.

```
00007FF7575816D4  74 CE  je simplecrackme.7FF7575816A4
00007FF7575816D4  75 CE  jne simplecrackme.7FF7575816A4
```

Now assembly instructions are looks like this. So, I've changed **JE** to **JNE** (**Jump if Not Equal**).



So, I will patch it using **CTRL+P** then save it as "**simplecrackme-cracked.exe**". So, let's execute our new PE file (Portable Execution file | .exe file).



So, it is successful. Now program has been cracked successfully. And it will open a YouTube link. We can also see that link while we looking for string.

Thank you for reading this writeup. Don't forget to follow me. Best regards, **Piyusha Akash. (0x3xp)**

Portfolio: https://0x3xp.github.io

LinkedIn: https://linkedin.com/in/piyushaakash

GitHub: https://github.com/0x3xp

Linktree: https://linktr.ee/piyushaakash